Navigating the Security Practice Landscape

Julia H. Allen, Software Engineering Institute [vita[1]]

2006-10-30

This article presents a summary of ten leading sources of security practice definition and implementation guidance. It uses ISO 17799 as a foundation (given its international standard status and broad, installed base) and builds on and augments it with additional source material. A summary of publicly available CERT course materials is presented to aid in practice implementation. The content in this article can be used independently or in concert with the approaches described in the other articles in this content area.

Introduction

Purpose

The intent of this article is to provide a navigational aid through the leading sources of security standards, frameworks, and guidelines, at a more detailed level than the other articles in this content area. We'll look at various standards as well as CERT courseware that can help you better understand *how to implement* these standards.

You need not read this content from A to Z; instead, you can focus first on those practices or standards that you wish to implement immediately and then later delve into those you might not have considered before. We recommend using this article as a reference and a guide.

Contents

This article

- describes the benefit of using a defense-in-depth or layered defense approach to deploying and operating security practices
- presents a summary of the leading sources of security practice definition and implementation guidance
- uses ISO 17799 [ISO 05a[2]] as a foundation and builds on and augments it with additional source material
- summarizes publicly available CERT courseware that provides detailed, how-to implementation guidance, including online lectures and labs

Publicly Available Documents Describing Security Practices

Many publicly available and useful frameworks, guidelines, and sets of practices describe actions organizations should take to deploy and operate secure systems and deliver secure services to their customers. These include

- the Payment Card Industry Security Standard[3]
- publications[4] provided by the U.S. National Institute of Standards and Technology (NIST) for U.S.

1. daisy:215 (Allen, Julia H.)

2. daisy:583#ISO05a (Deployment & Operations References)

3. https://www.pcisecuritystandards.org/tech/index.htm

federal agencies

- community-based frameworks such as
  - ITIL[5] for the IT service management industry
  - COBIT[6] for the IT governance and IT audit communities [ITGI 05a[7]], [Campbell 05[8]]
  - publications developed by BITS[9] and the Federal Financial Institutions Examination Council (FFIEC[10]) [FFIEC 06[11]] for the U.S. financial services sector
  - the American Chemistry Council's Responsible Care® Program[12] for the chemical industry [ACC 02[13]], [ACC 06[14]]
  - member-organization-based frameworks such as the Information Security Forum's *Standard of Good Practice for Information Security*[15] [ISF 05]
- user/vendor consensus frameworks such as the Center for Internet Security[16]'s consensus configuration benchmarks for specific operating systems and other technologies
- international standards, most notably ISO/IEC 17799 [ISO 05a[17]], ISO/IEC 27001 [ISO 05b[18]], ISO/IEC 20000 [ISO 05c[19]], and ISO 21827 [ISO 04[20]]

Adoption of any of these, in concert with a commitment to continuous improvement, appears, at least anecdotally,[21] to achieve and sustain an improved level of operational security.

Defense in Depth

Such a wealth of security practices can be overwhelming to review, understand, and use as a basis for determining what to do. One effective means for navigating the security practices landscape is to implement a layered defense or defense-in-depth strategy (refer to the BSI Defense in Depth principle[23] description).[24]

NIST Special Publication 800-27

NIST Special Publication 800-27, *Engineering Principles for Information Technology Security* [Stoneburner 04[26]] states that

Securing information systems against the full spectrum of threats requires the use of multiple, overlapping protection approaches addressing the people, technology, and operational aspects of information systems. This is due to the highly interactive nature of the various systems and networks and the fact that any single system cannot be adequately secured unless all interconnecting systems are also secured.

By using multiple, overlapping protection approaches, the failure or circumvention of any individual protection approach will not leave the system unprotected. Through user training and awareness, well-crafted policies and procedures, and redundancy of protection mechanisms, layered protections enable effective protection of information technology for the purpose of

4. http://csrc.nist.gov/publications/fips/index.html

5. http://www.ogc.gov.uk/index.asp?id=2261

6. http://www.itgi.org/

7. daisy:583#ITGI05a (Deployment & Operations References)

8. daisy:583#Campbell05 (Deployment & Operations References)

9. http://www.bitsinfo.org/

10. http://www.ffiec.gov/ffiecinfobase/html_pages/it_01.html

11. daisy:583#FFIEC06 (Deployment & Operations References)

12. http://www.responsiblecare-us.com/

13. daisy:583#ACC02 (Deployment & Operations References)

14. daisy:583#ACC06 (Deployment & Operations References)

15. http://www.isfsecuritystandard.com/index_ns.htm

16. http://www.cisecurity.org/

17. daisy:583#ISO05a (Deployment & Operations References)

18. daisy:583#ISO05b (Deployment & Operations References)

19. daisy:583#ISO05c (Deployment & Operations References)

20. daisy:583#ISO04 (Deployment & Operations References)

22. daisy:583#IsecT06 (Deployment & Operations References)

21. Refer to the web sites noted above. See also [IsecT 06[22]] for a description of additional security-related standards.

23. daisy:347 (Defense in Depth)

25. daisy:583#Hazle06 (Deployment & Operations References)

24. See also [NSA] and [Hazlewood 06[25]].

26. daisy:583#Stone04 (Deployment & Operations References)

achieving mission objectives.

As part of **Principle 8**: Implement tailored system security measures to meet organizational security goals, NIST 800-27 states:

> Recognizing the uniqueness of each system allows a layered security strategy to be used – implementing lower assurance solutions with lower costs to protect less critical systems and higher assurance solutions only at the most critical areas.

As part of **Principle 16**: Implement layered security (ensure no single point of vulnerability), NIST 800-27 goes on to state

> For example, the use of a packet-filtering router in conjunction with an application gateway and an intrusion detection system combine to increase the work-factor an attacker must expend to successfully attack the system.

> The need for layered protection is especially important when commercial off-the-shelf (COTS) products are used.

Redundancy and Diversity

Two of the key architectural approaches to consider as part of a layered defense are redundancy[27] and diversity. "**Redundancy** says you have more than one of everything, **diversity** says you have more than one of everything but they're different. If you can do some redundancy and some diversity where, for example, you distribute your infrastructure in multiple physical locations, then the motivated attacker has to think harder about what part of your organization they're going to target" [Lindner 06[30]].

Another example is to operate both Linux and Windows operating systems on critical servers such that if one is attacked, the other is not affected. Clearly there are **risks, tradeoffs, and costs** to consider in implementing such a strategy. Redundancy and diversity solutions are typically more expensive and require additional staff skill and competence. These **costs** need to be weighed against the **benefit** of fewer or less disruptive security breaches and the ease of restoring a system to its production state after it has been compromised.

Plan, Do, Check, Act[31], Risk-Centered Practices[32], and Integrating Security and IT[33] provide additional guidance on how to select practices that can aid in implementing a defense-in-depth approach.

Security Practice Categorization

This section presents categories of security practices to consider during deployment and operations. Its intent is to serve as a navigational aid through the leading sources of security practices and frameworks,

---

28. http://en.wikipedia.org/wiki/Defense_in_depth

29. daisy:583#Lindner06 (Deployment & Operations References)

27. "Defense-in-depth[28] may mean an engineering solution which emphasizes redundancy—a system that keeps working even when a single component fails—over attempts to design components that will not fail in the first place" [Lindner 06[29]].

30. daisy:583#Lindner06 (Deployment & Operations References)

31. daisy:574 (Plan, Do, Check, Act)

32. daisy:575 (Risk-Centered Practices)

33. daisy:576 (Integrating Security and IT)

---

at a more detailed level than the other articles in this content area.

Given widespread, international use, ISO 17799 *Code of practice for information security management* [ISO 05a[34]] and ISO 27001 Annex A *Information security management systems* [ISO 05b[35]] were used to build the initial master list of practices categories. Categories were then expanded and updated based on the additional sources described below.

Some of the practice categories (such as managing human resources and managing the physical environment for security) are well beyond the scope of deployment and operations. They are included here for completeness; several (such as acquire and develop secure systems) are addressed in much greater detail in other BSI content areas.

The practice categories are as follows. Table 1[36] (available at the end of this article) identifies subpractices within these categories and sources that provide further details, including guidance for practice implementation in support of secure deployment and operations.

- Assess, manage, and mitigate security risk.
- Develop, review, and maintain a useful security policy.
- Develop, review, and maintain a useful security plan.
- Manage the organization to operate securely, including both internal operations and relationships with external parties.
- Adequately protect organizational assets that have security requirements and affect the security of the enterprise.
- Manage human resources for security prior to employment, during employment, and following changes in assignment or termination.
- Manage the physical environment to meet security requirements and mitigate risk.
- Ensure the correct and secure operation of systems and software. This includes a wide range of practices such as change management, configuration management, third party service delivery, system planning, dealing with malicious code, backup, network security, and all forms of monitoring and security assessment.
- Control access to all classes of assets in support of business requirements.
- Acquire, develop, and maintain secure systems. For the purposes of deployment and operations, this includes vulnerability management and change management.
- Report and manage security incidents.
- Ensure business continuity.
- Comply with legal requirements and other sources of security requirements.

Sources Used to Identify Practice Categories

The following sources were used in constructing the security practice categories described above and expanded in Table 1[37]. They contain security practice definitions and system- and software-neutral implementation guidance:

- ISO/IEC 17799[38]

---

34. daisy:583#ISO05a (Deployment & Operations References)

35. daisy:583#ISO05b (Deployment & Operations References)

36. #tbl1

37. #tbl1

38. #17799

- [ISO/IEC 27001](#27001)[39]
- [COBIT](#COBIT)[40]
- [Corporate Information Security Working Group](#CISWG)[41]
- [Information Security Forum](#ISF)[42]
- [ITIL](#ITIL)[43]
- [NIST special Publication 800-27](#800-27)[44]
- [NIST Special Publication 800-53](#800-53)[45]
- [Security in the Software Lifecycle](#Lifecycle)[46]
- [VISA U.S.A. Payment Application Best Practices](#VISA)[47]
- [CERT Courseware](#CERT)[48]

ISO/IEC 17799

Code of practice for information security management [ISO 05a[49]] describes 11 security domains and addresses compliance with these domains at managerial, organization, legal, operational, and technical levels. The eleven domains include

- security policy
- organization of information security
- asset management
- human resources security
- physical and environmental security
- communications and operations management
- access control
- information systems acquisition, development, and maintenance
- information security incident management
- business continuity management
- compliance

ISO/IEC 27001

Information security management systems [ISO 05b[50]] describes a model for developing and managing an effective Information Security Management System (ISMS). This model is based on the Plan-Do-Check-Act (PDCA) approach commonly used in other quality models. This standard defines the certification requirements for demonstrating compliance with ISO 17799 and comprises both documentation and implementation audits. More information on this standard is available in [Plan, Do, Check, Act](#)[51].

COBIT®

Control Objectives for Information and related Technologies [ITGI 05a[52]][53] describes a framework for

39. #27001

41. #CISWG

42. #ISF

43. #ITIL

44. #800-27

45. #800-53

46. #Lifecycle

47. #VISA

48. #CERT

49. daisy:583#ISO05a (Deployment & Operations References)

50. daisy:583#ISO05b (Deployment & Operations References)

51. daisy:574 (Plan, Do, Check, Act)

52. daisy:583#ITGI05a (Deployment & Operations References)

53. See also http://en.wikipedia.org/wiki/COBIT.

IT governance. It is intended to ensure the effectiveness, efficiency, confidentiality, integrity, availability, compliance, and reliability of information and the systems used to process information. COBIT is organized into

- four domains (planning and organization; acquisition and implementation; delivery and support; and monitoring)
- 34 high-level control objectives
- 318 detailed control objectives

Refer to Integrating Security and IT[55] for more details on COBIT.

Corporate Information Security Working Group

The Corporate Information Security Working Group (CISWG) was convened by Representative Adam Putnam (R-FL) and met from November 2003 through November 2004. The CISWG Phase II Best Practices and Metrics Team had as its **goal** to "develop a resource that would help Board members, managers, and technical staff establish their own comprehensive structure of principles, policies, processes, controls, and performance metrics to support the people, process, and technology aspects of information security" [CISWG 04[56]].

Information Security Program Elements

This team's Phase II report[57] gives detailed descriptions of Information Security Program Elements (ISPE) for governance, management, and technical operations. While these elements define security metrics, each metric relies on the presence of one or more **security practices** against which measures are collected, analyzed, and reported. The report defines 99 metrics. Appendices describe a baseline set of 65 that organizations can use to get started and a smaller subset of 40 for small and medium enterprises.

Governance ISPEs are discussed in the BSI Governance & Management[58] content area. Management and Technical ISPEs are relevant to deployment and operations and are listed in Table 2[59]. Refer to the report for a detailed description of each of these elements.

Table 2. CISWG Information Security Program Elements

Management	- ISPE8 Establish Information Security Management Policies and Controls and Monitor Compliance - ISPE9 Assign Information Security Roles, Responsibilities, and Required Skills, and Enforce Role-based Information Access Privileges - ISPE10 Assess Information Risks, Establish Risk Thresholds, and Actively Manage Risk Mitigation - ISPE11 Ensure Implementation of Information

55. daisy:576 (Integrating Security and IT)

56. daisy:583#CISWG04 (Deployment & Operations References)

57. http://www.educause.edu/LibraryDetailPage/666&ID=CSD3661

58. daisy:549 (Governance & Management)

59. #table2

	Security Requirements for Strategic Partners and Other Third Parties
	• ISPE12 Identify and Classify Information Assets
	• ISPE13 Implement and Test Business Continuity Plans
	• ISPE14 Approve Information Systems Architecture During Acquisition, Development, Operations, and Maintenance
	• ISPE15 Protect the Physical Environment
	• ISPE16 Ensure Internal and External Audits of the Information Security Program with Timely Follow-up
	• ISPE17 Collaborate with Security Staff to Specify the Information Security Metrics to be Reported to Management
Technical	• ISPE18 User Identification and Authentication
	• ISPE19 User Account Management
	• ISPE20 User Privileges
	• ISPE21 Configuration Management
	• ISPE22 Event and Activity Logging and Monitoring
	• ISPE23 Communications, Email, and Remote Access Security
	• ISPE24 Malicious Code Protection, Including Viruses, Worms, and Trojans
	• ISPE25 Software Change Management, including Patches
	• ISPE26 Firewalls
	• ISPE27 Data Encryption
	• ISPE28 Backup and Recovery
	• ISPE29 Incident and Vulnerability Detection and Response
	• ISPE30 Collaborate with Management to Specify the Technical Metrics to be Reported to Management

Information Security Forum

The Information Security Forum is an international association of over 280 organizations (including 50 per cent of Fortune 100 companies) that fund and cooperate in conducting practical research in information security.

The ISF's *Standard of Good Practice for Information Security* [ISF 05[60]] provides "a set of high-level

---

60. daisy:583#ISF05 (Deployment & Operations References)

principles and objectives for information security together with associated statements of good practice." This guideline is organized into **five aspects,** each of which covers a particular type of operational environment. These include

- security management
- critical business applications
- computer installations
- networks
- systems development

"*Computer installations* and *networks* provide the underlying infrastructure on which the *critical business applications* run. *Systems development* deals with how new applications are created, and *security management* addresses high-level direction and control" [ISF 05[61]].

Each aspect comprises multiple areas (30 in all) as shown in Table 3[62]. Each area comprises multiple sections (135 in all). Each section is described by a principle, an objective, and multiple practices.

Table 3. ISF aspects and areas

SM Security Management	SM1 high level direction
	SM2 security organization
	SM3 security requirements
	SM4 secure environment
	SM5 malicious attack
	SM6 special topics
	SM7 management review
CB Critical Business Applications	CB1 security requirements
	CB2 application management
	CB3 user environment
	CB4 system management
	CB5 local security management
	CB6 special topics
CI Computer Installations	CI1 installation management
	CI2 live environment
	CI3 system operation
	CI4 access control
	CI5 local security management
	CI6 service continuity

61. daisy:583#ISF05 (Deployment & Operations References)

62. #table3

NW Networks	NW1 network management
	NW2 traffic management
	NW3 network operations
	NW4 local security management
	NW5 voice networks
SD Systems Development	SD1 development management
	SD2 local security management
	SD3 business requirements
	SD4 design and build
	SD5 testing
	SD6 implementation

The final appendix of this Standard provides a matrix of topics that cut across and map to the aspects, areas, and sections. Twenty-six pages of topics are listed in alphabetical order, including availability, business requirements, change management, encryption, passwords, risk analysis, security audit/review, and vulnerabilities.

ITIL

ITIL documents a set of **12 processes** that include high-level overviews as well as detailed definitions of the steps in each process [ITIL 00[63]], [ITIL 01[64]].

ITIL processes include

- configuration management
- change management
- incident management
- problem management
- release management
- service-level management
- service reporting
- availability management
- service continuity management
- security management
- capacity management
- financial management

ITIL process definitions describe the service management process as defined in ISO/IEC 20000 *Information technology – Service management* [ISO 05c[65]] and as depicted in Integrating Security and

---

63. daisy:583#ITIL00 (Deployment & Operations References)

64. daisy:583#ITIL01 (Deployment & Operations References)

65. daisy:583#ISO05c (Deployment & Operations References)

IT[66].

NIST Special Publication 800-27

Engineering Principles for Information Technology Security [Stoneburner 04[67]] identifies 33 "system-level security principles to be considered in the design, development, and operation of an information system. These principles are also helpful in affirming and confirming the security posture of an already deployed information system." Nineteen of these are essential to achieving and sustaining the desired security posture during deployment and operations. The 800-27 principle numbers are retained here for ease of traceability:

- Principle 2: Treat security as an integral part of the overall system design.
- Principle 5: Reduce risk to an acceptable level. (See Risk-Centered Practices[68].)
- Principle 6: Assume that external systems are insecure.
- Principle 7: Identify potential tradeoffs between reducing risk, increased costs, and decreased operational effectiveness (reworded to be more clear).
- Principle 8: Implement tailored system security measures to meet organizational security goals.
- Principle 9: Protect information while being processed, in transit, and in storage.
- Principle 13: Use common language in developing security requirements. (This principle is necessary for evaluating and comparing security products, features, and their performance.) (See BSI Requirements Engineering[69] content area.)
- Principle 14: Design security to allow for regular adoption of new technology, including a secure and logical technology upgrade process.
- Principle 15: Strive for operational ease of use.
- Principle 16: Implement layered security[70] (ensure no single point of vulnerability).
- Principle 17: Design and operate an IT system to limit damage and to be resilient in response.
- Principle 18: Provide assurance that the system is, and continues to be, resilient in the face of expected threats.
- Principle 21: Use boundary mechanisms to separate computing systems and network infrastructures.
- Principle 23: Develop and exercise contingency or disaster recovery procedures to ensure appropriate availability.
- Principle 24: Strive for simplicity.
- Principle 25: Minimize the system elements to be trusted.
- Principle 26: Implement least privilege.
- Principle 32: Authenticate users and processes to ensure appropriate access control decisions both within and across domains.
- Principle 33: Use unique identities to ensure accountability.

NIST Special Publication 800-53

Recommended Security Controls for Federal Information Systems [Ross 06[71]] "provides guidelines for selecting and specifying security controls for information systems supporting the executive agencies of

66. daisy:576 (Integrating Security and IT)

67. daisy:583#Stone04 (Deployment & Operations References)

68. daisy:575 (Risk-Centered Practices)

69. https://buildsecurityin.us-cert.gov/daisy/bsi/articles/best-practices/requirements.html

70. #did-l2

71. daisy:583#Ross06 (Deployment & Operations References)

the federal government. It applies to all components of an information system that process, store, or transmit federal information."

Categories of Security Controls

This guideline identifies management, operational, and technical classes of controls in the following categories. The numbers in parentheses are the number of specific controls in each category.

- AC access control (20)
- AT awareness and training (5)
- AU audit and accountability (11)
- CA certification, accreditation, and security assessments (7)
- CM configuration management (7)
- CP contingency planning (10)
- IA identification and authentication (7)
- IR incident response (7)
- MA maintenance (6)
- MP media protection (6)
- PE physical and environmental protection (19)
- PL planning (6)
- PS personnel security (8)
- RA risk assessment (5)
- SA system and services acquisition (11)
- SC system and communications protection (23)
- SI system and information integrity (SI)

Mappings to Other Standards

Appendix G Security Control Mappings provides a detailed mapping of 800-53 controls to **ISO 17799** paragraphs.

Appendix H Standards and Guidance Mappings provides a detailed mapping of 800-53 controls to all other relevant **NIST Special and FIPS publications**.

NIST 800-53 "associates recommended minimum security controls with **FIPS 199** [NIST 03[72]] low-impact, moderate-impact, and high-impact security categories" [Ross 06[73]]. Annex 1 of this publication describes a baseline set of minimum security controls for low-impact information systems, Annex 2 for moderate, and Annex 3 for high.

Security in the Software Lifecycle

Security in the Software Lifecycle: Making Software Development Processes – and Software Produced by Them – More Secure [Goertzel 06[74]] "describes methodologies, life cycle process models, sound practices, and supporting technologies that have been reported to increase the likelihood that the

---

72. daisy:583#NIST03 (Deployment & Operations References)

73. daisy:583#Rogers04 (Deployment & Operations References)

74. daisy:583#Goertzel06 (Deployment & Operations References)

---

resulting software will be free of exploitable faults." With respect to deployment and operations, this report recommends the following practices, using the names Distribution and Sustainment for these life cycle phases:

- Distribution
  - Clean up code before distribution to
    - remove debugger hooks and other developer backdoors
    - remove hard-coded credentials
    - remove sensitive comments in user-viewable code
    - remove unused calls
    - remove pathnames to unreferenced, unused, or hidden files
    - remove data-collecting trapdoors
    - reconfigure default accounts and groups
    - replace relative pathnames
  - Set configuration defaults as restrictively as possible.
  - Implement trusted distribution techniques (such as code signatures or authentication of download links) to prevent or make evident tampering with distributed code.
- Sustainment
  - Perform impact assessments and address unacceptable impacts for all patches before distribution.
  - Use software rejuvenation and reconfiguration techniques to prevent vulnerabilities that emerge due to software ageing.

These practices are described in more detail in Appendices G.7 and G.8.

Visa U.S.A. Payment Application Best Practices

In addition to the Payment Card Industry Data Security Standard [PCI 06[75]] discussed in Plan, Do, Check, Act[76], Visa has developed a set of payment application best practices [Visa 06[77]]. The purpose of these practices is to assist software vendors of payment applications to develop and deploy products that are more secure and are compliant with the PCI standard.

The following practices are relevant to deploying and operating secure software. Each practice description includes detailed subpractices and testing procedures for verifying that the practice is in place.

- Practice 3: Provide secure password features.
- Practice 4: Log application activity.
- Practice 6: Protect wireless transmissions.
- Practice 7: Test applications to address vulnerabilities.
- Practice 8: Facilitate secure network implementation.
- Practice 10: Facilitate secure remote software updates.
- Practice 11: Facilitate secure remote access to applications.

---

75. daisy:583#OGC05 (Deployment & Operations References)

76. daisy:574 (Plan, Do, Check, Act)

77. daisy:583#VISA06 (Deployment & Operations References)

- Practice 12: Encrypt sensitive traffic over public networks.
- Practice 13: Encrypt all non-console administrative access.

CERT Courseware[78]

Author: Stephanie Losi[79]

This section describes three CERT courses that focus on information assurance:

- Information Assurance Defense-in-Depth: Foundations for Secure and Resilient IT Enterprises[80]
- Survivability and Information Assurance Curriculum[81]
- Virtual Training Environment[82]

Defense-in-Depth: Foundations for Secure and Resilient IT Enterprises

The Defense-in-Depth Foundational Curriculum [May 06[83]] can bring a big-picture perspective to the often detail-focused world of computer and network security, while reinforcing concepts with some implementation details.

Target Audience

The curriculum is designed for students, ranging from system administrators to CIOs, who have some technical understanding of security and want to better understand how security issues affect their entire organization. It can be useful for system administrators and IT security personnel who would like to step up to the management level. It also can provide a refresher for IT managers and executives who want to stay up-to-date on the latest technological threats facing their enterprise.

Instructors should be familiar with both the technical and managerial aspects of security and should have significant real-world experience so they can relate anecdotes as well as present curriculum material. Students should be familiar with basic computer networking and should have an interest not only in learning technological details but also in placing those details within a larger business context.

Curriculum Content

The curriculum consists of eight modules plus an introduction called "Foundations of Information Assurance." This introduction focuses on how addressing the overarching concepts of confidentiality, integrity, and availability can lead to a comprehensive security strategy.

The **eight modules** in the curriculum are

1. Compliance Management
2. Risk Management
3. Identity Management
4. Authorization Management
5. Accountability Management
6. Availability Management
7. Configuration Management
8. Incident Management

78. http://www.cert.org/nav/index_gold.html
79. daisy:592 (Losi, Stephanie)
80. #did
81. #sia
82. #vte
83. daisy:583#May06 (Deployment & Operations References)

The Compliance Management and Risk Management modules are presented at a fairly conceptual level; the remaining modules are presented at a more detailed level, while still preserving the big picture.

Module Descriptions

Each module is divided into several subsections.

Compliance Management is presented as "the lynchpin of security." This section discusses U.S. laws, the need for executive-level support for security efforts, best practices for writing policies, and methods for increasing awareness of security policies throughout the organization. The Sample Policies section provides a pointer to examples and discusses techniques for creating effective policies.

Risk Management defines the concept of an asset and discusses how organizations can identify, categorize, and protect their assets using a defined process. Risks to assets must be identified and then ranked so that mitigation strategies can be put in place in a way that makes sense and supports the business mission.

Identity Management begins by defining various methods of user and computer identification as well as methods of authentication. It then moves on to discuss methods for protecting identity and privacy.

Authorization Management discusses the pros, cons, and best practices of file-system access control and network-traffic access controls. It also covers application-layer access controls, such as TCP wrappers and proxy servers.

Accountability Management defines accountability as a goal that is achieved through logging and auditing, network monitoring, and intrusion detection. Some of the subtopics discussed include automated availability checking, traffic monitoring and sniffing, antivirus, and integrity monitoring.

Availability Management presents the concepts of reliability, redundancy, failover, and fault tolerance, and then discusses various levels of availability that may be considered acceptable by organizations. Single points of failure are discussed, along with ways to mitigate them and ensure availability and business continuity.

Configuration Management details four methods of managing IT configurations: software update process, inventory control, configuration change management, and internal system assessments (such as penetration testing). Pros and cons and best practices are discussed.

Incident Management takes a process-based approach and covers planning and practice exercises, disaster and recovery preparation, and security incident handling and response.

Survivability and Information Assurance Curriculum

The SIA Curriculum[84] [CERT 05[85]] is useful if your organization approaches IT issues in a technology-centered way but would like to take a more process-centered approach. It helps organize system administration activities, going from a tactical, fire-fighting approach to a long-term, strategic approach.

The material contained in the SIA curriculum can be applied to sharpen system administrators' enterprise-level perspective and help system administrators and managers speak each other's language. As such, the SIA curriculum can be a useful tool for bridging the gap that often exists between technology-centered and process-centered approaches to IT.

Target Audience

---

84. http://www.cert.org/sia/

85. daisy:583#CERT05 (Deployment & Operations References)

Students are expected to have at least one to two years of experience in a system administration or closely related role. Instructors are intended to be experienced system administrators or managers of system administrators so that they can refer to real-world anecdotes as well as provided course materials.

Curriculum Description

The **key foundations** of the SIA curriculum are

1. Use the 10 Principles of Survivability and Information Assurance (listed below).
2. Understand that the network supports the core business mission—it is not technology for technology's sake.
3. Consider implementing Survivable Functional Units (explained below) to reduce network complexity and increase modularity.
4. Learn to build on existing enterprise networks.
5. Challenge assumptions.

Three courses form the curriculum.

1. The first course focuses on the 10 Principles of Survivability and Information Assurance[86] and is designed so that system administrators and their immediate managers can attend together.
2. The second course, "Information Assurance Networking Fundamentals[87]," applies the 10 principles from Course 1 to the inner workings of the TCP/IP suite. It is geared toward experienced system administrators.
3. The third and last course is titled "Sustaining, Improving, and Building Survivable Functional Units[88] (SFUs)." It is designed to integrate all of the information learned in the previous two courses.

Course 1: 10 Principles of Survivability and Information Assurance

This course is taught at a relatively high level but requires some competence with system administration tasks on any operating system. The course itself uses Red Hat Linux 9. There are discussions and a lab. The 10 Principles[89] [Rogers 04[90]] covered in the class are

1. Survivability is an enterprise-wide concern.
2. Everything is data.
3. Not all data is of equal value to an enterprise; risk must be managed.
4. Information assurance policy governs actions.
5. Identification of users, computer systems, and network infrastructure components is critical.
6. Survivable Functional Units (SFUs) are a helpful way to think about an enterprise's networks.
7. Security Knowledge in Practice (SKiP) provides a structured approach.
8. The road map guides implementation choices (all technology is not equal).
9. Challenge assumptions to understand risk.
10. Communication skill is critical to reach all constituencies.

The goal of the course is to apply these 10 principles to understand and solve system administration problems.

Course 2: Information Assurance Networking Fundamentals

Students review TCP/IP networking fundamentals outside of class using the book *TCP/IP Illustrated, Volume 1: The Protocols* [Stevens 93[91]]. In class, students

---

86. #course1
87. #course2
88. #course3
89. http://www.cert.org/archive/pdf/SIAPrinciples.pdf
90. daisy:583#Rogers04 (Deployment & Operations References)

- take quizzes on the readings,
- participate in a lab exercise, and
- discuss the TCP/IP suite, taking a view that challenges assumptions about networking features and attempts to identify the real-world limitations of the protocols.

The **goal** is to teach students to think like hackers but not act like them.

Course 3: Sustaining, Improving, and Building Survivable Functional Units (SFUs)

The premise is that students

- individually analyze artifacts on an existing network to determine its components
- work in teams to reengineer an existing functional unit of that network, based on the lessons learned in the first two courses
- give a class presentation to explain how they made the functional unit more survivable

Lastly, in an optional third section of the course, teams of students design, build, and graft a new SFU onto an existing enterprise network in a lab environment. This is a situation that many system and network administrators will encounter in their working lives.

The lab for this portion of the curriculum is currently theoretical, but organizations that think this course could serve their needs are encouraged to use the detailed design document provided along with the faculty course materials to build a lab environment.

Course Materials

Course materials, including 2800+ pages of student workbook content, can be downloaded from the curriculum web site[92].

Virtual Training Environment

CERT's Virtual Training Environment (VTE), as presented to the public, is a broad collection of more than 400 modules[93]. Modules may be documents, demonstrations with voiceovers, lecture videos with accompanying slides and notes, or labs.

Many topics are covered within VTE, and content is updated quarterly, so the best approach is to browse the site for the most current offerings. VTE is self-guided, so students who find the content to be of use can continue to explore various areas to gain additional knowledge.

Key **goals** of the VTE environment are to

- improve information security awareness worldwide
- provide a globally available training platform that improves the efficacy of online training efforts in information, computer, network, and system security

Target Audience

The VTE target audience consists of system administrators who are new to security or the security role and are seeking a reference library. They have technical backgrounds but possess varying degrees of security knowledge in topics such as forensics, incident handling, TCP/IP, and firewalls.

Instructors looking for material to supplement the courses they teach also may find VTE of value.

---

91. daisy:583#Stevens93 (Deployment & Operations References)

92. http://www.cert.org/sia/

93. https://www.vte.cert.org/pdf/VTE_Library_Content_List.pdf

Regardless of their job role, students should have some knowledge of computer and networking technologies on Windows and/or Linux, a healthy curiosity about how security technologies work, and a willingness to use the VTE material as a jumping-off point for further study. Simply pointing and clicking through the labs may be instructive, but the best results will be obtained by in-depth, authorized practice of the skills taught.

VTE Modules

This is a sampling of VTE content modules:

- Basics of Router Administration
- SSL and TLS
- Introduction to Log File Analysis Using SWATCH
- Steganography
- Compliance Management

Lab modules require a VTE subscription, but all other content is available to the public at no cost. To view audiovisual content, students will need the Adobe Flash plug-in.

CERT Course Material Available Via VTE

Some of the modules within the main VTE list are part of larger courses and are prefaced by various tags. These are the larger courses, along with a sampling of their associated modules:

- ISFTS - Information Security for Technical Staff
  - o Policy Formulation and Implementation
  - Securing Network Infrastructure
  - TCP/IP Security
  - Asset and Risk Management

- AISFTS - Advanced Information Security for Technical Staff
  - Synchronization and Remote Logging
  - Host System Hardening
  - Intrusion Detection
  - Firewalls and Access Controls

- FRGCF - First Responder's Guide to Computer Forensics
  - Cyber Law
  - File Systems/First Responder's Toolkit
  - Collecting Volatile Data
  - Collecting Persistent Data

- ADVFOR - Advanced Forensics
  - Capturing a Running Process
  - Configuration and Setup of Online DFS
  - Logfile Analysis Using Microsoft Log Parser
  - Bookmarking with EnCase

Additional VTE Content

Other tracks are available to paying subscribers and are presented in a more organized way:

- the Information Assurance Practitioner track, which contains a wide range of technical material
- a track geared toward Cisco-based networks, which is far more detailed
- a forensics track

Lastly, with a **training subscription**, organizations are able to combine material from the VTE platform with material from their own repositories to generate customized training courses.

Conclusion

The intent of this article has been to serve as a navigational aid through the wide range of available security standards, guidelines, and frameworks. We presented categories of security practices to consider during deployment and operations, drawing from leading sources. The content in this article can be used independently or in concert with the approaches described in the other articles in this content area.

Table 1: Security Practice Categories

Given their widespread, international use, ISO 17799 *Code of practice for information security management* [ISO 05a[94]] and ISO 27001 Annex A *Information security management systems* [ISO 05b[95]], described above, were used to build the initial master list of practices categories in Table 1[96]. Table entries were then expanded and updated based on additional sources, which are also described in more detail above.

Table 1. Security practice categories

Practice Category	Subpractice	Source
Assess, manage, and mitigate security risk.	Assess, manage	- Risk-Centered Practices[97] article - NIST 800-27 *Engineering Principles for Information Technology Security* [Stoneburner 04[98]], Principles 5, 7 - NIST 800-53 *Recommended Security Controls for Federal Information Systems* [Ross 06[99]], RA (risk assessment) "Report of the Best Practices and Metrics Teams", ISPE10 (assess risks) [CISWG 04[100]] - COBIT 4.0, PO9 (assess, manage IT risks) [ITGI 04[101], ITGI 05a[102]] *The Standard of Good Practice for Information*

94. daisy:583#ISO05a (Deployment & Operations References)

95. daisy:583#ISO05b (Deployment & Operations References)

96. #tbl1

97. daisy:575 (Risk-Centered Practices)

98. daisy:583#Stone04 (Deployment & Operations References)

99. daisy:583#Ross06 (Deployment & Operations References)

100. daisy:583#CISWG04 (Deployment & Operations References)

101. daisy:583#ITGI04 (Deployment & Operations References)

102. daisy:583#ITGI05a (Deployment & Operations References)

		Security SM3 (security requirements) [ISF 05[103]]
	Mitigate	• BSI principles Defense in Depth[104], Failing Securely[105], Securing the Weakest Link[106] • NIST 800-27, Principle 16 (defense in depth), 18 (resilience) • CISWG ISPE10 (manage risk mitigation) • COBIT DS5 (ensure systems security) • ISF CB4 (application resilience), CI2 (computer installation resilience), NW1 (network resilience)
Develop, review, and maintain a useful security policy.		• NIST 800-27, Principles 2, 8 • NIST 800-53 (all) • CISWG ISPE8 (establish policy) • ISF SM1 (high level direction)
Develop, review, and maintain a useful security plan.		• COBIT PO1 (define strategic IT plan), PO5 (manage IT investment), DS1 (define, manage service levels), DS5 (ensure systems security) • ITIL (service level, financial management)
Manage the organization to operate securely.	Management commitment to security	• ISF SM1 (high level direction)
	Internal organization	• NIST 800-27, Principles 2, 8, 15 • NIST 800-53 (all) • CISWG ISPE9 (assign roles, determine skills) • COBIT PO4 (define IT processes), PO6 (communicate), PO10 (manage projects) • ISF SM2 (security organization)
	External parties	• NIST 800-27, Principles 13, 15

103. daisy:583#ISF05 (Deployment & Operations References)

104. https://buildsecurityin.us-cert.gov/daisy/bsi/articles/knowledge/principles/347.html

105. https://buildsecurityin.us-cert.gov/daisy/bsi/articles/knowledge/principles/349.html

106. https://buildsecurityin.us-cert.gov/daisy/bsi/articles/knowledge/principles/356.html

		• NIST 800-53 RA (risk assessment) • ISF SM6 (third party access, outsourcing)
Adequately protect organizational assets.	Assign responsibility and ownership	• NIST 800-53 RA (risk assessment) • CISWG ISPE12 (identify, classify assets) • COBIT PO2 (define the information architecture), DS9 (manage the configuration) • ITIL (configuration, asset management) [ITIL 99[107]] • ISF SM3 (security requirements), SM4 (asset management)
	Classify assets	• BSI Principle Promoting Privacy[108] • NIST 800-27, Principle 9 • FIPS 199 *Security Categorization of Federal Information and Information Systems* [NIST 03[109]] • CISWG ISPE12 (identify, classify assets) • COBIT PO2 (define the information architecture) • ITIL (configuration, asset management) • ISF SM3 (security requirements), SM4 (privacy, asset management)
Manage human resources for security.	Prior to employment	• NIST 800-53, PS (personnel security) • COBIT PO7 (manage IT human resources) • ISF SM1 (high level direction)
	During employment	• NIST 800-27, Principle 15 • NIST 800-53, AT (awareness, training) • COBIT PO7 (manage IT human resources), DS7 (educate, train users)

107. daisy:583#ITIL99 (Deployment & Operations References)

108. https://buildsecurityin.us-cert.gov/daisy/bsi/articles/knowledge/principles/353.html

109. daisy:583#NIST03 (Deployment & Operations References)

		• ISF SM2 (security organization)
	Termination or change	• NIST 800-53, PS (personnel security)
Manage the physical environment to meet security requirements and mitigate risk.	Secure areas	• NIST 800-53, PE (physical, environmental protection) • CISWG ISPE15 (protect physical environment) • COBIT DS12 (manage the physical environment) • ISF SM4 (physical protection)
	Equipment	• NIST 800-53, CP (contingency planning), PE (physical, environmental protection) • CISWG ISPE15 (protect physical environment) • COBIT DS12 (manage physical environment) • ISF SM6 (equipment for remote use)
Ensure the correct and secure operation of systems and software.	Operational procedures (change management; segregation of duties, facilities)	• NIST 800-53, CM (configuration management), MA (maintenance) • COBIT AI4 (enable operation, use), AI6 (manage changes), DS13 (manage operations) • ITIL (configuration, change, release management) • CISWG ISPE21 (configuration management), ISPE 22 (communications, email, remote access), ISPE25 (change management) • Visa U.S.A. *Payment Application Best Practices,* Practice 10 (secure remote software updates) [Visa 06[110]] • ISF SM5 (patch management)
	Third party service delivery	• NIST 800-27, Principle 13 • NIST 800-53, CM

110. daisy:583#VISA06 (Deployment & Operations References)

		(configuration management), SA (system, services acquisition) • CISWG ISPE11 (security requirements for third parties) • COBIT DS1 (define, manage services levels), DS2 (manage third party services) • ITIL (service level management)
	System planning (capacity management, system acceptance)	• NIST 800-27, Principle 14, 15 • NIST 800-53, CP (contingency planning), PL (planning), SC (system and communication protection) • COBIT AI7 (accredit solutions and changes), DS3 (manage performance, capacity) • ITIL (capacity management) • ISF CI2 (installation design)
	Malicious and mobile code (such as automated tools)	• NIST 800-53, SC system and communications protection), SI (system and information integrity) • COBIT DS5 (ensure systems security) • CISWG ISPE24 (malicious code) • ISF SM5 (malicious code)
	Back-up	• NIST 800-53, CP (contingency planning) • COBIT DS4 (ensure continuous service), DS11 (manage data) • ITIL (availability, service continuity management) • CISWG ISPE28 (backup, recovery)
	Network security, including wireless	• BSI principles Never Assuming that Your Secrets Are Safe[111], Reluctance to

111. daisy:352 (Never Assuming that Your Secrets Are Safe)

		Trust[112]
		• NIST 800-27, Principles 6, 9, 21
		• NIST 800-53, SC (system and communication protection)
		• COBIT DS5 (ensure systems security)
		• CISWG ISPE26 (firewalls)
		• Visa Practice 6 (protect wireless transmissions)
	Media handling	• BSI Principle Promoting Privacy[113]
		• NIST 800-27, Principle 9
		• NIST 800-53, MP (media protection)
		• ISF SM4 (privacy)
	Exchange of information (includes instant messaging)	• BSI Principle Promoting Privacy[114]
		• NIST 800-27, Principle 9
		• NIST 800-53, MP (media protection), SC (system and communications protection)
		• COBIT PO8 (manage quality), DS5 (ensure systems security)
		• ISF SM4 (privacy), SM6 (instant messaging)
	Electronic commerce	• BSI Principle Promoting Privacy[115]
		• NIST 800-27, Principles 9, 17, 32
		• NIST 800-53, SC (system and communications protection)
		• COBIT AI4 (enable operation and use)
		• ISF SM6 (e-commerce)
	Monitoring, reporting	• BSI principle Never Assuming that Your Secrets Are Safe[116], Reluctance to Trust[117]
		• NIST 800-27, Principles 6, 18

112. daisy:355 (Reluctance to Trust)
113. daisy:353 (Promoting Privacy)
114. daisy:353 (Promoting Privacy)
115. daisy:353 (Promoting Privacy)
116. daisy:352 (Never Assuming that Your Secrets Are Safe)
117. daisy:355 (Reluctance to Trust)

		• NIST 800-53, AU audit and accountability), CA (certification, accreditation, and security assessments) • COBIT DS5 (ensure systems security), ME1 (monitor and evaluate IT performance) • ITIL (capacity, performance management) • CISWG ISPE17 (report management metrics), ISPE30 (report technical metrics), ISPE22 (logging, monitoring) • Visa Practice 4 (application logging) • ISF SM5 (intrusion detection), SM7 (monitor, review)
Control access to all classes of assets in support of business requirements.		• BSI principles Complete Mediation[118], Least Common Mechanism[119], Least Privilege[120], Never Assuming that Your Secrets Are Safe[121], Psychological Acceptability[122], Reluctance to Trust[123], Separation of Privilege[124] • CISWG ISPE9 (enforce role-based access privileges) • COBIT DS5 (ensure systems security)
	Business requirements	• NIST 800-27, Principle 26 • NIST 800-53, AC (access control)
	User access	• NIST 800-27, Principles 26, 32, 33 • NIST 800-53, AC (access control), IA (identification and authentication), PS (personnel security) • CISWG ISPE18 (user identification, authentication), ISPE19 (user account management), ISPE20 (user privileges)
	User responsibilities	• NIST 800-53, AC (access

118. daisy:346 (Complete Mediation)

119. daisy:350 (Least Common Mechanism)

120. daisy:351 (Least Privilege)

121. daisy:352 (Never Assuming that Your Secrets Are Safe)

122. daisy:354 (Psychological Acceptability)

123. daisy:355 (Reluctance to Trust)

124. daisy:357 (Separation of Privilege)

		control)
	Network access, including remote, wireless access	• NIST 800-27, Principles 6, 21, 25, 32 • NIST 800-53, AC (access control), CA (certification, accreditation, and security assessments) • ISF SM6 (remote access), NW2 (wireless access)
	Operating system access	• NIST 800-27, Principles 32, 33 • NIST 800-53, AC (access control), IA (identification and authentication)
	Application, information access	• NIST 800-27, Principle 25 • NIST 800-53, CM (configuration management) • Visa Practice 3 (application passwords), Practice 11 (secure remote access to applications)
	Mobile computing	• NIST 800-27, Principles 6, 32, 33 • NIST 800-53, AC (access control), PE (physical and environmental protection)
Acquire, develop, and maintain secure systems. [This topic is treated more comprehensively in other BSI content areas.]		• CISWG ISPE14 (approve systems architecture, full life cycle) • COBIT PO8 (manage quality), AI2 (acquire, maintain application software), AI3 (acquire, maintain technologies), AI5 (procure IT resources) • *Security in the Software Lifecycle*, Appendices G.7, G.8 [Goertzel 06[125]] • ISF SM4 (security architecture) • ISF SD1 (development management), SD2 (security management), SD3 (business requirements), SD4 (design, build), SD5 (test), SD6 (implement)

125. daisy:583#Goertzel06 (Deployment & Operations References)

	Security requirements	• BSI Requirements Engineering[126] content area • NIST 800-27, Principles 2, 13 • NIST 800-53, SA (system and services acquisition) • COBIT PO1 (define IT strategic plan), PO2 (define information architecture), AI1 (identify automated solutions)
	Correct processing in applications	• BSI Code Analysis[127], Coding Practices[128], Coding Rules[129] content areas • NIST 800-53, SI (system and information integrity)
	Cryptographic controls	• NIST 800-27, Principles 32, 33 • NIST 800-53, SC (system and communications protection) • COBIT DS5 (ensure systems security) • CISWG ISPE27 (data encryption) • Visa Practice 12 (encrypt sensitive traffic over public networks), Practice 13 (encrypt all non-console administrative access) • ISF SM6 (cryptography, public key infrastructure)
	Security of system files	• NIST 800-27, Principles 14, 32 • NIST 800-53, CM (configuration management) • COBIT DS9 (manage the configuration) • ITIL (configuration management)
	Security in development, support processes	• NIST 800-27, Principles 2, 14 • NIST 800-53, CM (configuration management), SA (system and services acquisition), SI (system and

126. daisy:67 (Requirements Engineering)

127. daisy:62 (Code Analysis)

128. daisy:75 (Coding Practices)

129. daisy:76 (Coding Rules)

		information integrity)
	Vulnerability management	• BSI principle Economy of Mechanism[130], Never Assuming that Your Secrets Are Safe[131], Securing the Weakest Link[132] • NIST 800-27, Principles 24, 25 • NIST 800-53, RA (risk assessment), SI (system and information integrity) • COBIT AI6 (manage changes) • ITIL (change, release management) • CISWG ISPE25 (change management), ISPE29 (vulnerability detection) • Visa Practice 7 (test for vulnerabilities) • ISF SM5 (patch management)
	Application is able to operate in a secure environment	• Visa Practice 8 (secure network implementation)
Report and manage security incidents.	Report	• BSI Incident Management[133] content area • NIST 800-53, IR (incident response) • COBIT DS4 (ensure continuous service), DS5 (ensure systems security), DS8 (manage service desk, incidents), DS10 (manage problems) • ITIL (incident, problem management) • CISGW ISPE29 (incident response)
	Manage	• BSI Incident Management[134] content area • BSI principle Failing Securely[135] • NIST 800-27, Principles 17, 18 • NIST 800-53, AU (audit and accountability), IR (incident

130. daisy:348 (Economy of Mechanism)

131. daisy:352 (Never Assuming that Your Secrets Are Safe)

132. daisy:356 (Securing the Weakest Link)

133. daisy:64 (Incident Management)

134. daisy:64 (Incident Management)

135. daisy:349 (Failing Securely)

		response)
		• COBIT DS4 (ensure continuous service), DS5 (ensure systems security), DS8 (manage service desk, incidents), DS10 (manage problems)
		• ITIL (incident, problem management)
		• CISGW ISPE29 (incident response)
		• ISF SM5 (emergency response)
	Forensic investigations	• ISF SM5 (forensics)
Ensure business continuity.		• BSI principle Failing Securely[136]
		• NIST 800-27, Principles 17, 18, 23
		• BSI Governance & Management[137] content area
		• CERT PrISM work [Caralli 05[138], Caralli 06[139]]
		• NIST 800-53, CP (contingency planning), IR (incident response), RA (risk assessment)
		• CISWG ISPE13 (implement, test business continuity plans)
		• COBIT DS4 (ensure continuous service)
		• ITIL (service continuity, availability management)
		• ISF SM4 (business continuity), CI6, NW3 (service continuity)
Comply with security requirements.	With legal requirements	• BSI Principle Promoting Privacy[140]
		• NIST 800-27, Principle 9
		• NIST 800-53, AU (audit and accountability), CA (certification, accreditation, and security assessments), (all policy sections)
		• CISWG ISPE8 (monitor compliance)

136. daisy:349 (Failing Securely)

137. daisy:549 (Governance & Management)

138. daisy:583#Caralli05 (Deployment & Operations References)

139. daisy:583#Caralli06 (Deployment & Operations References)

140. daisy:353 (Promoting Privacy)

		• BSI Governance & Management[141] content area • COBIT ME3 (ensure regulatory compliance), DS9 (manage the configuration) • ISF SM4 (privacy)
	With security policies, standards	• ensure compliance with all BSI principles[142] • NIST 800-27, Principle 18 • NIST 800-53, CA (certification, accreditation, and security assessments) • CISWG ISPE8 (monitor compliance) • COBIT ME2 (monitor and evaluate internal control)
	Audit	• NIST 800-27, Principle 18 • NIST 800-53 AU (audit and accountability), PL (planning) • CISWG ISPE16 (ensure audits) • COBIT ME1 (monitor and evaluate IT performance), ME2 (monitor and evaluate internal control), ME3 (ensure regulatory compliance) • ISF SM6 (audit)

Terms of Use

Responsible Care® Program is registered in the U.S. Patent and Trademark office by the American Chemistry Council.

CERT® and CERT Coordination Center® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

COBIT® is registered in the U.S. Patent and Trademark office by the Information Systems Audit and Control Association and by the IT Governance Institute.

The IT Infrastructure Library® and ITIL® are registered trademarks of the British Office of Government Commerce (OGC). ITIL was developed in conjunction with the British Standards Institute and is overseen by The IT Service Management Forum[143] (itSMF).

141. daisy:59 (Governance & Management)

OCTAVE® is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

142. daisy:79 (Principles)

143. http://www.itsmf.com/

Operationally Critical Threat, Asset, and Vulnerability Evaluation[SM] is a service mark of Carnegie Mellon University.

SKiP[SM] is a service mark of Carnegie Mellon University.

Carnegie Mellon Copyright

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

Fields

Name	Value
Copyright Holder	SEI

Fields

Name	Value
is-content-area-overview	false
Content Areas	Best Practices/Deployment & Operations
SDLC Relevance	Deployment
Workflow State	Publishable
Sort Order	10

---

1.   http://www.sei.cmu.edu/about/legal-permissions.html